Elektrotehnički fakultet
Banja Luka

Mrežno i distribuirano programiranje
08.09.2020.

1. **(50)** *HideMe* je klijent-server aplikacija koja pruža svojim učesnicima mogućnost razmjene ključeva za kriptovanu komunikaciju na steganografski način (parametri potrebni za generisanje ključeva skriveni su u tekstualnom fajlu). Dva klijenta, Alisa i Bob, vrše razmjenu tekstualnog fajla preko socket servera na sljedeći način:
    a. Alisa se prijavljuje na server unosom korisničkog imena, nakon čega joj server vraća poruku THERE_IS_A_FILE_FOR_YOU**(1)**, u slučaju da je dobila fajl od Boba, ili THERE_IS_NO_FILE**(2)**, u slučaju da razmjena fajlova tek treba da počne. U slučaju **(1)**, Alisa šalje poruku DOWNLOAD kako bi joj se prikazao sadržaj fajla; pored prikaza, iz fajla je potrebno izdvojiti riječ koja se nalazi u trećoj liniji fajla i prikazati je spojenu sa dužinom primljenog fajla – ova sekvenca predstavlja ključ. Osim toga, potrebno je uporediti riječ sa onom koju je Alisa očekivala kao odgovor. U slučaju **(2)**, Alisa šalje serveru poruku UPLOAD, nakon čega mu prosljeđuje tekstualni fajl koji je prethodno kreirala i u koji je u treću liniju upisala tajno pitanje. Zbog provjere autentičnosti samog fajla, na Bobovoj strani je uvijek potrebno provjeravati da li treća linija završava sa znakom **?**, i u slučaju da linija ne završava navedenim karakterom potrebno je raskinuti komunikaciju sa serverom. Alisa kreira fajl odmah nakon pokretanja aplikacije kroz komandnu liniju. Prikazuje joj se poruka za unos sadržaja fajla liniju po liniju (minimalno mora unijeti 5 linija), a kad završi sa unosom sadržaja, fajl sačuvati kao *alisa.txt*. Nakon toga, Alisa unosi i odgovor na pitanje koje je postavila i koje se sačuva u fajl *odgovor.txt*.
    b. Bob se prijavljuje na server unosom korisničkog imena, nakon čega mu server vraća poruku THERE_IS_A_FILE_FOR_YOU**(1)**, u slučaju da je dobio fajl od Alise, ili THERE_IS_NO_FILE**(2)**. U slučaju **(1)** Bobu se prikazuje sadržaj fajla i zatim posebno treća linija fajla, nakon čega Bob mora da unese odgovor na pitanje; nakon unosa odgovora, pitanje u trećoj liniji fajla se mijenja odgovorom, te se novokreirani fajl prosljeđuje nazad na server; nakon slanja se na Bobovoj strani prikazuje odgovor spojen sa dužinom novokreiranog fajla. U slučaju **(2)** konekcija sa serverom se raskida.

    Napomena: Kao dokaz o uspješnoj razmjeni ključeva, sa izvornim kodom zadatka potrebno je predati i *screenshot* na kom su prikazani ispisi razmjenjenih ključeva na komandnoj liniji.

2. **(50)** Napraviti jednostavnu klijentsku konzolnu aplikaciju kod koje korisnik unosi sa tastature samo jednu naredbu od četiri moguće: 1) SUM *a*, *b*, *c* 2) GET DATE 3) SAVE *filename text* 4) READ *filename*. Na osnovu unesenih vrijednosti, poziva se jedna od četiri metode RMI serverskog objekta. Prve dvije metode prave odgovarajući zahtjev prema REST servisu, a odgovor nakon obrade vraća se klijentskom objektu. Treća i četvrta metoda se obrađuju na RMI serveru. Treća metoda serijalizuje dobijeni tekst u Kryo formatu (strukturu proizvoljno definisati) u fajl sa proslijeđenim imenom, a četvrta deserijalizuje fajl sa proslijeđenim imenom i vraća sačuvani tekst. Ako fajl ne postoji, vratiti odgovarajuću grešku.

    REST dio ima metodu koja sabira *n* brojeva i vraća odgovor u JSON formatu: {result: “number”, action: “sum”}. Druga metoda vraća trenutno vrijeme u JSON formatu: { result: “dd.MM.yyyy”, action: “date”}. Kada RMI serverski objekat dobije odgovor, tada parsira JSON objekat i klijentu vraća samo datum ili samo rezultat sabiranja brojeva (result *polje*). Dobijeni rezultati se prikazuju na klijentskoj konzolnoj aplikaciji.

Vrijeme rada: 180 minuta